UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
BEAUMONT DIVISION

Angela Steinhardt, *Plaintiff*, v. albertAI.click, *et al.*, *Defendants*.	Case No. 1:25-cv-00303-MJT **Declaration of Evan Cole**

I, Evan Cole, state and swear as follows.

I. Introduction

1. My name is Evan Cole. I am of sound mind and capable of making this Declaration. I have personal knowledge of the facts stated herein.

2. I am the Head of Investigations at The Hoda Law Firm, PLLC. I am experienced in blockchain investigations and am knowledgeable about the pig-butchering scam epidemic and the tactics of cybercriminals like the Defendants in this case. I hold the Chainalysis Cryptocurrency Fundamentals and Chainalysis Reactor Certifications, and the Lukka Crypto Asset Investigation I Certification.

II. Pig-Butchering Scams

3. I have reviewed the Complaint in this matter and Plaintiff's Motion for Preliminary Injunction (the "Motion"). Based on my training and experience, after reviewing these materials, I have concluded that Dr. Steinhardt was the victim of what is known as a "pig-butchering scam."

4. I have attached a report from Proofpoint, a leading cybersecurity firm, as Exhibit 1-A to this Declaration.[1] This report details the employment-scam variant of pig-butchering fraud. Dr. Steinhardt's case is a direct analog to the cases discussed in the study, as evidenced by the method of initial contact, the "phases" in which the scam progressed, the degree of emotional engineering involved, and the nature of the fraudulent employment platform used to legitimize the scam, which are all detailed further in Plaintiff's Complaint and the instant Motion. Comparison of the facts of Dr. Steinhardt's case to the Proofpoint report confirms that Dr. Steinhardt was the victim of an employement-related crypto scam here.

III. Blockchain Tracing

5. I performed a blockchain tracing investigation into the flow of Dr. Steinhardt's funds after their transfer to the scammers' blockchain addresses. This investigation revealed that (i) $100,800.00 of Dr. Steinhardt's

[1] Tim Kromphardt, *et al.*, *Pig Butchers Join the Gig Economy: Cryptocurrency Scammers Target Job Seekers*, PROOFPOINT, available at: https://www.proofpoint.com/us/blog/threat-insight/pig-butchers-join-gig-economy-cryptocurrency-scammers-target-job-seekers (published Oct. 28, 2024).

assets were ultimately transferred to deposit addresses at the Bitget cryptocurrency exchange, (ii) approximately $170,000.00 of Dr. Steinhardt's assets were ultimately transferred to deposit addresses at the Binance cryptocurrency exchange, and (iii) $20,000.00 of Dr. Steinhardt's assets were ultimately transferred to deposit addresses at the Coinbase cryptocurrency exchange. A blockchain tracing report which shows Dr. Steinhardt's funds traceable to the Bitget and Coinbase exchanges is attached as Exhibit 1-B to this Declaration. A blockchain tracing graph showing the flow of Dr. Steinhardt's funds to Binance is attached as Exhibit 1-C to this Declaration.

IV. Risk of Transfer

6. Pig-butchering victims have a fleeting opportunity to seek to freeze misappropriated assets shortly after the scam concludes. The process of laundering ill-gotten gains takes time, and usually requies cybercriminals to move at least some of the victim's assets through accounts at cryptocurrency exchanges that may comply with U.S. court orders and law-enforcement requests. But even where a victim's assets can be traced to identifiable cryptocurrency exchanges that would cooperate with freezing orders, those assets could be further dissipated at any moment, to non-compliant exchanges, to an unfreezable "self-custody" address, or "off ramped" by swapping them for fiat currency. Once stolen assets have been transferred in this way, recovery becomes highly unlikely.

[SIGNATURE PAGE FOLLOWS]

VERIFICATION

I, Evan Cole, hereby verify and declare under penalty of perjury that the foregoing is true and correct.

Evan Cole
Head of Investigations
The Hoda Law Firm, PLLC
evan@thehodalawfirm.com

July 7, 2025

www.proofpoint.com /us/blog/threat-insight/pig-butchers-join-gig-economy-cryptocurrency-sca…

Pig Butchers Join the Gig Economy: Cryptocurrency Scammers Target Job Seekers

10/23/2024

October 28, 2024 Tim Kromphardt, Genina Po, Hannah Rapetti, and Selena Larson

Key takeaways

- Proofpoint has observed an increase in cryptocurrency fraud that impersonates various organizations to target users with fake job lures.
- Researchers assess with high confidence this fraud is conducted by actors who conduct Pig Butchering, or romance-based cryptocurrency investment fraud.
- The job fraud has smaller but more frequent returns for the fraudsters compared to Pig Butchering.
- The activity leverages popular brand recognition in place of a long, romance-based confidence scam.
- The activity uses a flexible platform to tailor the scam to a variety of lure types.
- The activity is initiated through social media, SMS and messaging apps like WhatsApp and Telegram.

Overview

For years, Pig Butcher scammers have swindled victims out of billions of dollars. Typically, they lure victims in with long-winded confidence scams that eventually

direct victims to a fake cryptocurrency investment platform. Once a target's initial small investment starts turning into a large (but fake) "profit," the scammers pressure the victim to invest vast sums of money. Once the victim's money leaves their digital wallet, the unrealized gains are replaced with a sinking realization—they have lost everything.

While quite profitable for the pig butchers, these scams take a long time and offer many opportunities for the victim to realize something might be off. For this business model to be successful, they need to target victims with money to lose. This leaves a large market of financially insecure victims—that provide the scammers with smaller payout, but a larger pool of people—virtually untapped. Recently, however, Proofpoint observed these types of fraudsters launch a new business venture to tap into this market: job scamming.

In June 2024, the U.S. Federal Bureau of Investigation published a public service announcement warning the public of these fraudulent job scams originating on mobile devices.

Job duties may include

The scam typically begins with an unsolicited message on a social media platform or other messaging application, like SMS, WhatsApp, Telegram, etc. It starts out like a typical job recruiter message (see Figures 1 and 2). They specifically highlight the job as a work from home (WFH) opportunity. Despite recent pushes for return to office (RTO), remote jobs remain very popular with job seekers.

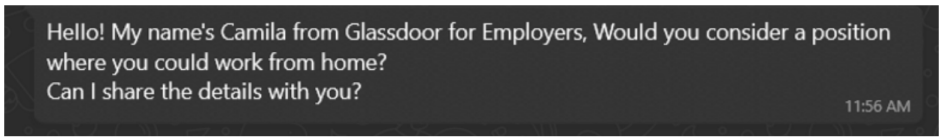


Figure 1: Fake Glassdoor recruiter.

The fraudster then launches into a brief description of the company "work platform." The specific job and brand impersonation can vary quite a bit from boosting popular music streams on Spotify to reviewing fake TikTok Shop products and services, or even giving hotel reviews. Essentially click farming.

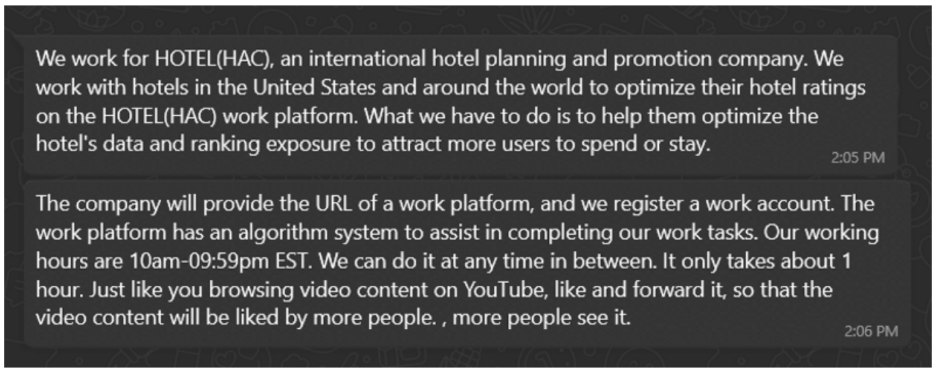


Figure 2: Hotel ratings job scam pitch.

Once the target agrees to take the job, the threat actor instructs them to register on a website, which is malicious. To register, the target is given a referral code. The page content is not viewable unless a user is registered. This makes surfacing and taking down these websites slightly more challenging for defenders, as domain takedown requests often require a substantial amount of evidence. Luckily, Emerging Threats was up to the challenge and has developed signatures to identify these new job scam sites.

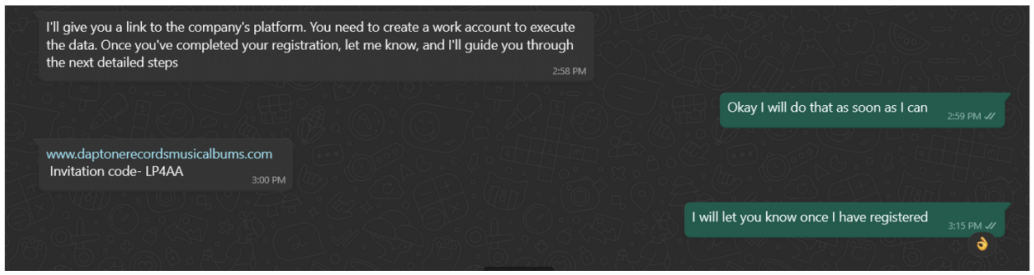


Figure 3: Directions to register.

After the victim has registered with the site, the job scammer—or "handler"—will ask that the target shares a screenshot of their profile page so they can create a training account.

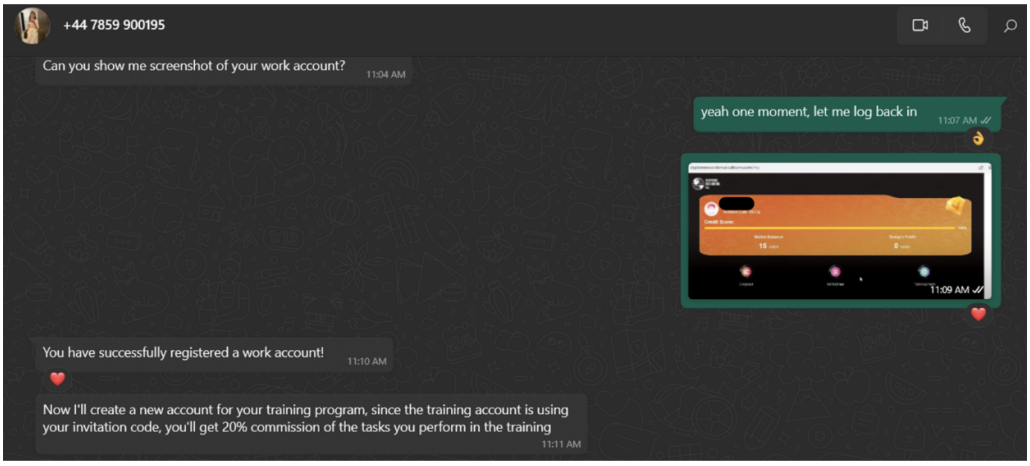


Figure 4. Request to share screenshot of profile page.

Gotta spend money to lose money

Once the training account has been created, the fraudster will instruct the recipient on how to perform their job function. This part will vary a bit depending on the platform theme—like submitting product or service reviews, placing product orders or booking hotels—but the core characteristics are the same. The user must click a button to submit a review, sales data, play music or some other task. The following is a list of impersonated companies and the "jobs" they attempted to recruit our researchers for:

Impersonated Company	Task Request
Outlier Ventures	Fake app store application reviews
Temu	Fake product reviews
TikTok	Fake product and purchasing reviews
Daptone Records	Fake streaming music reviews and playing specific songs via Spotify
Hotel Association of Canada	Fake hotel reviews and bookings

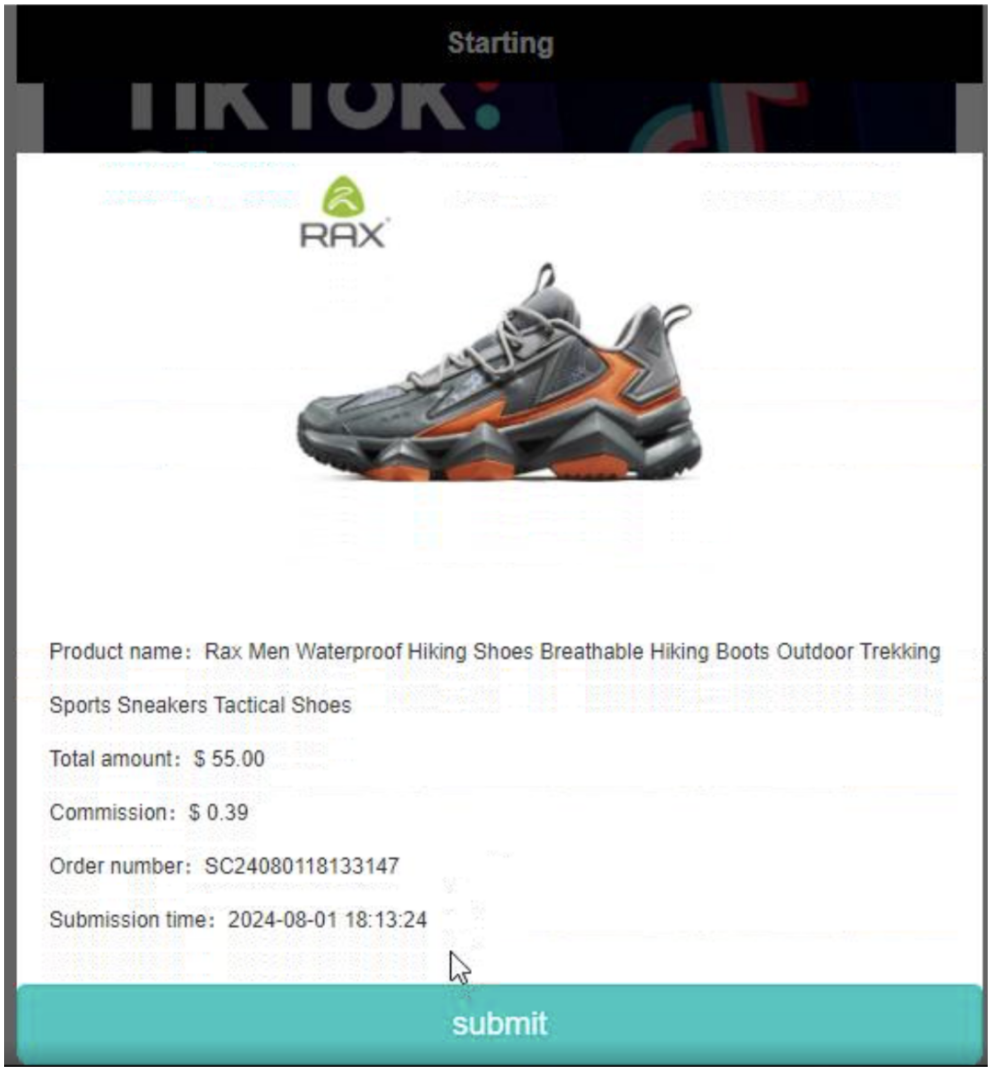


Figure 6: TikTok-Advance[.]com shopping data submission page. This is not affiliated with the social network TikTok.

The number of times a user must click to get "paid" will vary from 30-50 times per job session, based on instructions from their "handler." After clicking for a bit (usually a little over halfway through), the user will encounter an error that will not allow them to continue. The fake commission account balance will show a negative amount. The handler will explain that the user has encountered a "lucky" event and will be super jazzed.

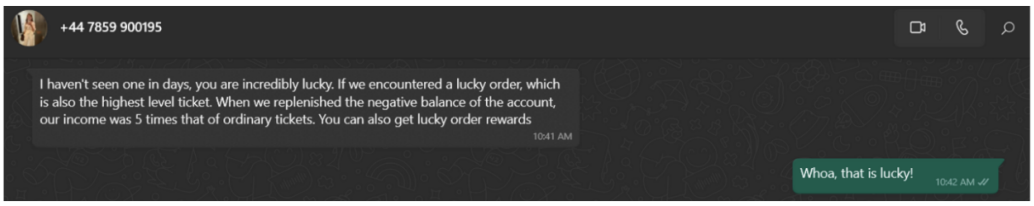


Figure 7: Lucky event.

The handler does not give a clear explanation as to why the account balance was reduced to zero, but claims it is good for the victim. The fraudster explains that once the user brings the account back out of the negative, they will unlock a multiplier on their income. For training, the handler will pay it this time, but the user will get to reap the rewards once they start on their own account. They will instruct the user to reach out to a support agent on the platform to get the cryptocurrency wallet address and they will bring the account out of the negative and ask that you continue your work. Once work has been completed, they will direct the user to log back into their own account. It will typically show a balance of $70 to $80. And if they try to start working again, the webpage with the fake account balance details will inform the user that to use the platform they will need to bring the account up to a minimum of $100. The handler will urge them to do so or lose out on the "5x bonus" received during training. The scammer will also inform the target about their "VIP commission tiers" (see Figure 8) where workers can invest between $100-$5,000 to increase the number of commissions received and how many tasks can be submitted in a day.

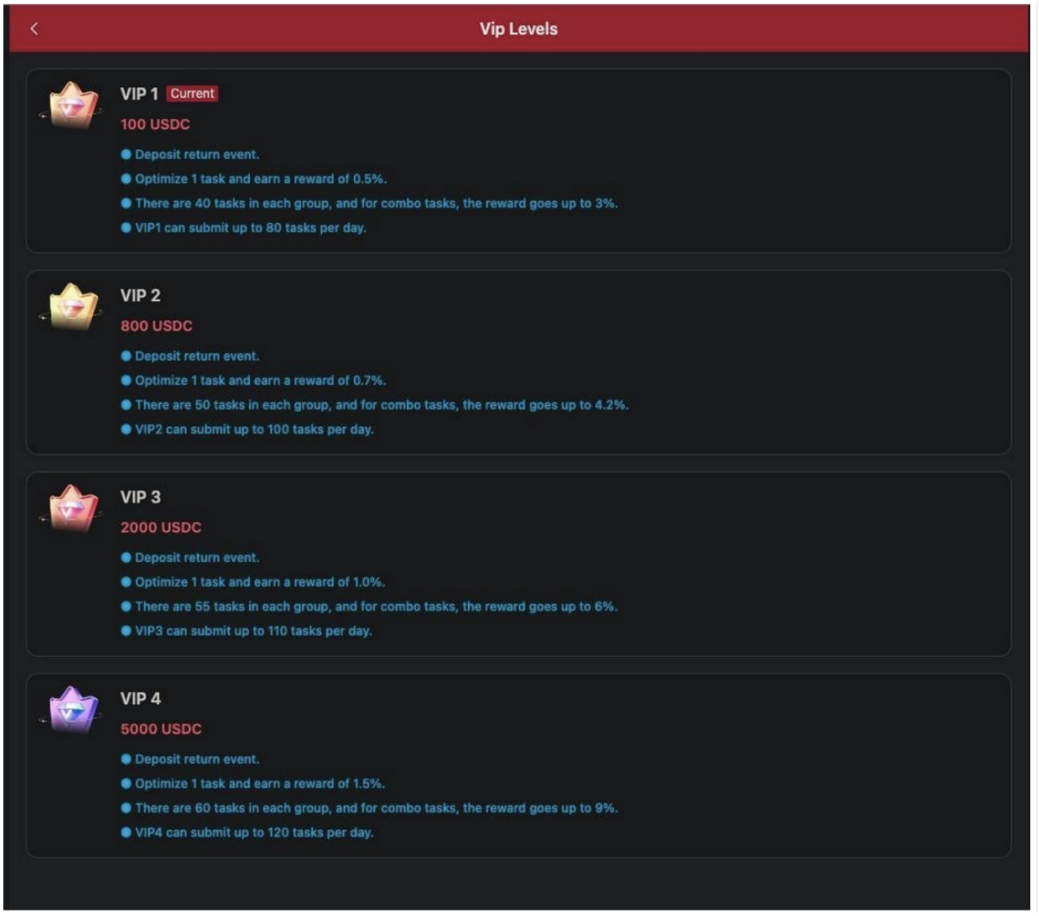


Figure 8: VIP multipliers.

Click, click, boom

So, what happens next? Let's assume the victim tops off the account using their own money and starts happily clicking away. After a couple days of building up their commission check, they will get "lucky" and have a negative balance again like in the training session. Their handler will urge them to pay into it and reassure them that it will be worth it. After sending the cryptocurrency to the designated wallet, the victim will indeed start seeing their balance start to climb as predicted. Much like the related Pig Butcher scam, at this point the victim may even be allowed to withdraw their first "paycheck." The withdrawal is never allowed to be more than they have put into the platform, but they will be allowed to take out some. The platforms do not process any payments. Instead, they are processed by the "customer service" reps or the handler (assuming the handler thinks they will continue to keep paying out, that is). This vicious cycle will continue as long as the scammers think the victim will keep paying into the system. If they suspect their victim has become wise to the scam, they will lock their account and ghost them. While losses are typically lower than your run-of-the-mill Pig Butcher cryptocurrency investment scam, losses can easily climb into the tens of thousands of dollars.

Danger in numbers

While many of these scams involve a one-on-one relationship between the victim and the handler, Proofpoint researchers have identified some victims being directed to a large group chat on Telegram or WhatsApp. This allows them to fill the chat with confederates who will gaslight the victims and brag about how much money they have made. We see this type of group chat frequently with Pig Butcher scams. If you are suddenly added to any group chat on these types of platforms, be very wary. Proofpoint researchers have observed the group and individual chats operating in multiple countries and languages.

"I would never fall for that!"

At first glance, this scam seems very unlikely to work. Having to pay a company money to get paid is absurd, you might think to yourself. But scams work because of emotions and desires. And for many job seekers, especially those in great need of an income, the prospect of a well-paying job with limited job requirements and seemingly quick payouts may seem alluring enough to ignore potential signs of a scam.

To get a better understanding of why and how people may fall for these scams, our threat researchers asked Proofpoint resident psychologist Dr. Bob Hausmann what factors are at play that could make the scam so effective. According to Dr. Hausmann, there are likely three psychological mechanisms at work:

1. Sunk cost fallacy
2. Loss aversion
3. Principle of reciprocity

The sunk cost fallacy is the idea that people will not abandon something or stop doing something when they have invested heavily in it, whether it be time or money, despite the investment not returning positive results. This concept, as part of the scam, is also fueled by what behavioral psychologists call loss aversion—the idea that the fear of losing outweighs the feeling of obtaining an equivalent amount of money. In this case, the job scam victim likely feels they have put too much time and effort into making a perceived sum, and so they will pay into the fake website in order to prevent the loss of what they believe to be hard-earned gains.

Additionally, whether they realize it or not, the scammer relies on the principle of reciprocity to get their target to pay into the fake platform. By paying the initial sum when the balance went below zero, the handler appears to do the target a favor by paying the negative balance, and then the target is indebted to them. In this case, the target is willing to go along with the next cycle and pay the negative balance themselves.

Unfortunately, all these psychological factors are part of why the scam is so successful.

According to our colleagues at the cryptocurrency investigation company Chainalysis, thousands of people have decided to pay into fake job platforms. Proofpoint researchers shared public cryptocurrency wallet addresses associated with identified job scams to see how effective the schemes were. Chainalysis' research showed that the cryptocurrency wallet for daptonerecordsmusicalbums[.]com—a fake job site impersonating a record label—had only been active for two months but made over $300,000 in Bitcoin and Ethereum. Funds from this wallet have been going into an account shared by short-term trade investment scams (aka Pig Butchers), and other job scam sites, according to Chainalysis' findings.

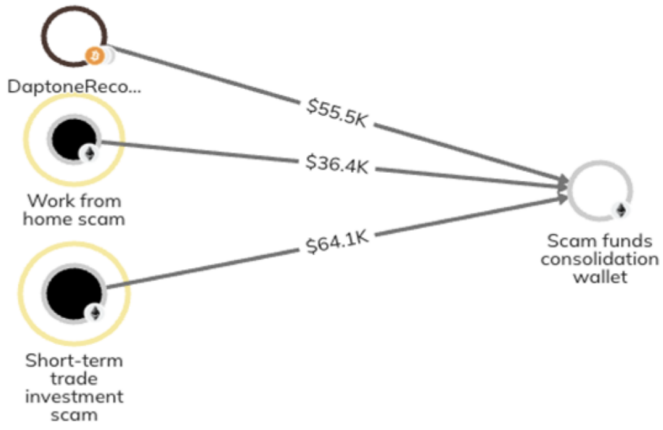


Figure 9: Pig Butcher and job scam cryptocurrency flow. In this case, the actors impersonated Daptone Records.

Here is a summary of how much cryptocurrency was stolen by the fake job scam websites identified by our researchers in collaboration with Chainalysis:

- hotelassociationseogp[.]com – 3K2t5GuZrZRByvVC1LuHUKrJ5LtKGJF7Mv: 80+ deposits were made in a month netting the scammers over $23,000.
- outlierventures-app[.]com - bc1qg9sz72jg3mptpmmqavjmqwq4dm3j5txpk0w0fu: 362 deposits over a single week totaling $95,000.
- temu-workbench[.]com - 3PZ1hqATmdncvuWUQaYfrLYXoRTMXres85: Over 1,000 deposits were made in a month totaling over $275,203.
- tiktok-advance[.]com - 0x3D2C12420D829D8AFc166C1632a4c54e7798F4fd: 130 deposits were made over a three-day period totaling over $80,000.

While this is a small sample size, it's clear that these job scamming groups are able to bring in substantial amounts of money via cryptocurrency in a short amount of time.

Conclusion

Cryptocurrency investment and job-related scams are extremely prevalent and use sophisticated social engineering techniques to convince people they are legitimate.

Just like confidence scammers have done for centuries, fraudsters continue to promise easy money to unsuspecting targets to swindle them.

To protect yourself, friends and family against these types of scams, Proofpoint recommends the following:

- Remain vigilant about unsolicited job offers, no matter the platform or application on which it is received. These fraudsters often use social media and SMS, but similar techniques have been observed in email as well.
- Never provide any money to a person who claims to be an employer. While this particular scam relies on the target paying into a fake job website, Proofpoint has observed other job scams that ask for payment for alleged goods and services like computer equipment to conduct advance fee fraud (AFF).
- Remember the old adage: If it seems too good to be true, it probably is.
- Spread the word. Knowledge is power when fighting scams.

Indicators of compromise

The Proofpoint Takedown Team, in collaboration with key providers, quickly neutralized the threats from the listed domains using a two-part mitigation process, offering rapid protection across global networks. If your organization is concerned about employees accessing these sites, Emerging Threats has added some new signatures to assist you.

2055539 - ET PHISHING PigButcher Kit Headers 2024-08-05

2055540 - ET PHISHING PigButcher Credential Phish Landing Page M1 2024-08-05

2055541 - ET PHISHING PigButcher Credential Phish Landing Page M2 2024-08-05

2055542 - ET PHISHING PigButcher Credential Phish Landing Page M3 2024-08-05

2055543 - ET PHISHING PigButcher Credential Phish Landing Page M4 2024-08-05

2055544 - ET PHISHING PigButcher Credential Phish Landing Page M5 2024-08-05

Indicator	Description
3K2t5GuZrZRByvVC1LuHUKrJ5LtKGJF7Mv	hotelassociationseogp[.]com BTC wallet
1M7kuP94Pv5DY7SPfyT5zfEXUeNCZDHg1t	daptonerecordsmusicalbums[.]com BTC wallet
0x2E65f3E0492e0a429D897521597bcc7Ec1CC4C9d	daptonerecordsmusicalbums[.]com ETH wallet
3PZ1hqATmdncvuWUQaYfrLYXoRTMXres85	temu-workbench[.]com BTC wallet
0x404c7c72e8869af9c617ad428fd2d2652f1cf298	outlierventures-app[.]com USDT
bc1qg9sz72jg3mptpmmqavjmqwq4dm3j5txpkowofu	outlierventures-app[.]com BTC
0x3D2C12420D829D8AFc166C1632a4c54e7798F4fd	tiktok-advance[.]com ETH
tcampaigns[.]vip	Malicious Domains

aprimo-data[.]life		
aprimo-world[.]life		
argoshop[.]shop		
argoshop[.]vip		
bandcampmusicalbumsseo[.]com		
bandcamponlinemusicmkt[.]com		
bandcampwebplayer[.]com		
onlinemusicdosbeatport[.]com		
beatportmusicdosgp[.]com		
bleepmusicspace[.]com		
bleepwebplayer[.]com		
bloomhouse-datagp[.]com		
bloomhouse-mktinc[.]com		
bloomingdales-digital[.]com		
bloomingdales-dos[.]com		
bloomingdalesseo[.]com		
1y1m[.]com		
cinkasuwashop[.]com		
brandasticdata[.]com		
buildingbrandsdos[.]com		
buildingbrandsmkt[.]com		
ppcchart-metric[.]com		
workchartmetric[.]com		
chart-metric-servicr[.]com		
zxjt9183[.]icu		
clicdata-data[.]life		
clicdata-work[.]life		
clutch-data[.]com		
clutch-pcp[.]com		
clutchppc[.]com		
clutch-ppc[.]com		
clutch-work[.]com		
cubixclickworker[.]com		
cubixdatagp[.]com		
cubixdosllc[.]com		
cubix-pcp[.]com		
cubix-player[.]com		
daptonemusicclub[.]com		
daptonerecordsgroupppromo[.]com		
daptonerecordsmusicalbums[.]com		

daptonerecordsppcgp[.]com		
daptonerecordspromohub[.]com		
daptonerecordspromotions[.]com		
daptonespace[.]com		
dayuse-ppc[.]com		
dayuse-seo[.]com		
searchhotelpricesdatainc[.]com		
searchhotelpricesdosgp[.]com		
deezer-albumsdata[.]com		
deezermusicdatappc[.]com		
devcommedia26[.]com		
dominoamusellc[.]com		
dominomusicdosllc[.]com		
dominomusicgp[.]com		
dominomusicgrouphub[.]com		
dominomusicpcpllc[.]com		
dominomusicpromotions[.]com		
dominomusicwebplayer[.]com		
ebaydatagp[.]com		
ebayseollc[.]com		
edifiandosgp[.]com		
edifianpcpinc[.]com		
edifianppcllc[.]com		
edifianseollc[.]com		
e-digitals-intelligence[.]com		
e-intelligence-data[.]com		
eintelligencejob[.]com		
eintelligencepcp[.]com		
e-intelligence-player[.]com		
e-intelligence-seo[.]com		
emubandsmusicspace[.]com		
emu-bands-player[.]com		
emusic-data[.]com		
emusic-ppc[.]com		
trip12345[.]top		
geniusmusicalbumsdata[.]com		
geniusmusicplayer[.]com		
gro-data[.]com		
gro-dos[.]com		
gro-pcp[.]com		

gummicube[.]top		
gummicube[.]xyz		
gummicubevip[.]com		
gummicubevip[.]cyou		
gummicubevip[.]top		
hometogo[.]cc		
hotelassociationdosinc[.]com		
hotelassociationseogp[.]com		
hotelplannerdatagp[.]com		
hotelplannerseoinc[.]com		
ig-plus[.]com		
ihutu[.]xyz		
imdbgp[.]com		
imdbmoviespromotions[.]com		
imdb-promotions[.]com		
imdbseollc[.]com		
ineffablemusicgrouphub[.]com		
ineffablemusicpromohub[.]com		
interpublicdata[.]com		
jango-data[.]com		
jangoppc[.]com		
jango-seo[.]com		
landmarktheatresdosgp[.]com		
landmark-theatres-ppc[.]com		
landmark-theatres-promo[.]com		
seolandmarktheatresinc[.]com		
lanternsoldata[.]com		
lanternsold-digital[.]com		
lanternsoldos[.]com		
lanternsold-pcp[.]com		
lanternsolppcgp[.]com		
lanternsolseoinc[.]com		
lastfmmusicspace[.]com		
lastfmwebplayer[.]com		
legendarycinemallc[.]com		
legendaryflim[.]com		
legensdarycin[.]com		
dosmylighthouse[.]com		
mylighthousedata[.]com		
livemusicppc[.]com		

liveonemusicalbumsppc[.]com		
liveoneonlinemusicservice[.]com		
liveone-ppc[.]com		
live-one-promo[.]com		
madisontaylormarketingdata[.]com		
amazon668[.]com		
livre19[.]com		
mer1996[.]com		
mer1998[.]com		
mer-live[.]com		
mer1998[.]cc		
mer-live[.]cc		
ma588[.]com		
mewsdosgp[.]com		
mgmmoviegrouphub[.]com		
mgmmoviepromohub[.]com		
miracledigital[.]ai		
miracledigital[.]vip		
miracledigitalinc[.]com		
miracledigitalseo[.]com		
mixcloudmusicgrouphub[.]com		
mixcloudmusicwebplayer[.]com		
motown-player[.]com		
motown-space[.]com		
buy0tw[.]store		
musicgateway-pcp[.]com		
musicgateway-seo[.]com		
musicoverygroupboost[.]com		
musicoverypromohub[.]com		
musicoverywebplayer[.]com		
onlinemusicppcmusicovery[.]com		
musiio-data[.]com		
musiio-player[.]com		
napster-promohub[.]com		
nspromalbums[.]com		
worknapster[.]com		
nytroseodata[.]com		
nytroseo-product[.]com		
olivineseo[.]com		
olivinework[.]com		

open-sea-club[.]com		
openseapromohub[.]store		
open-sea-space[.]com		
opensea-player[.]com		
padula-media-digital[.]com		
padula-mediapcp[.]com		
padula-mediaseo[.]com		
pandoragrouphub[.]com		
pandoramusicpromotions[.]com		
pandorapromohub[.]com		
perfechterproductions-data[.]com		
perfechterproductions-ppc[.]com		
perfechterproductions-seo[.]com		
paylist-push-ppc[.]com		
paylist-push-seo[.]com		
paylist-push-work[.]com		
playlistmusicspace[.]com		
playlist-push-ppc[.]com		
pod-bean-data[.]com		
pod-bean-player[.]com		
podbean-promotions[.]com		
podbean-space[.]com		
powerdigitalmarketingppc[.]com		
powerdigitalmarketingseo[.]com		
power-dos[.]com		
powermakerting-work[.]com		
power-pcp[.]com		
qobuzgrouphub[.]com		
qobuzpromohub[.]com		
radioplayer-data[.]com		
radioplayer-ppc[.]com		
rappppc[.]com		
rappseo[.]com		
datarioks[.]com		
rioksdata[.]com		
rioks-dos[.]com		
rioksdosgp[.]com		
rioksdosinc[.]com		
rioksdosllc[.]com		
rioks-mkt[.]com		

rioksmktllc[.]com		
riokspcpinc[.]com		
rioksppc[.]com		
rioks-ppc[.]com		
riokswork[.]com		
seorioks[.]com		
roveecomsdosllc[.]com		
sana-commerce-data[.]com		
sana-commerce-seo[.]com		
digitals-search-gather[.]com		
search-gather-data[.]com		
semrush-dos[.]com		
semrush-seo[.]com		
seoestoredata[.]com		
seoestoredosgp[.]com		
seoestoreppc[.]com		
seoestorework[.]com		
serviceware-world[.]life		
premersn[.]com		
sh-online[.]co		
datasolustar[.]com		
solustar-ppc[.]com		
solustar-seo[.]com		
solustarwork[.]com		
sonyrewardspro[.]net		
rcamusicgroupppromo[.]com		
rcamusicmktinc[.]com		
rcamusicmktllc[.]com		
rcamusicpromohub[.]com		
data-sound-click[.]com		
sound-click-ppc[.]com		
soundcloud-ppc[.]com		
soundcloud-seo[.]com		
soundhoundai-dos[.]com		
soundhoundai-seo[.]com		
spotmusicclickworker[.]com		
boomplaypromohub[.]com		
boomplaypromotions[.]com		
musictimegroupppromo[.]com		
musictimepromohub[.]com		

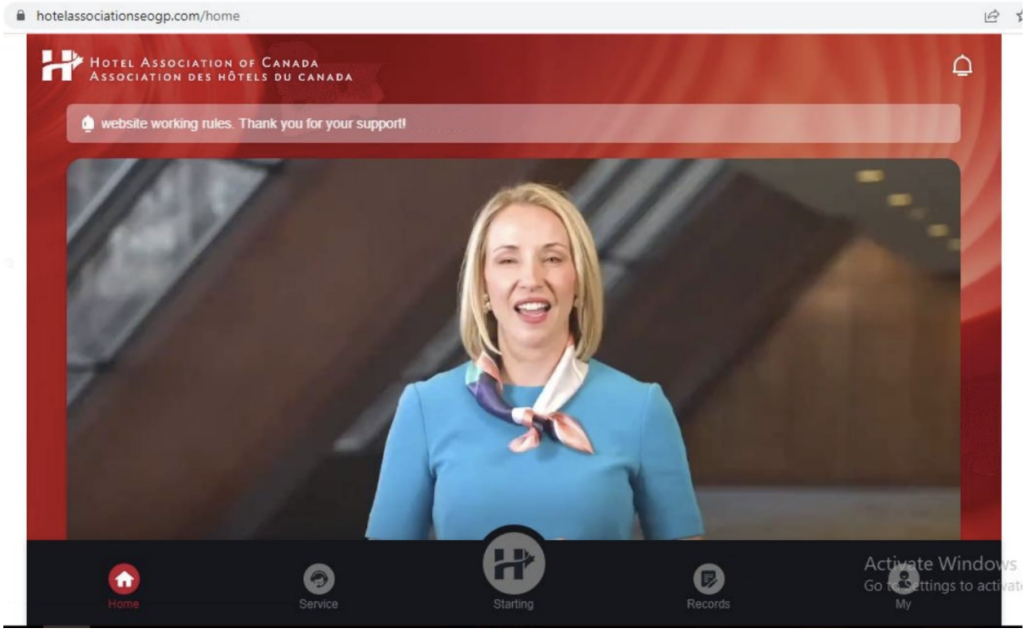
stingraymusicdata[.]com		
stingray-ppc-music[.]com		
stingray-space[.]com		
cbccentenr[.]net		
centralmarketing[.]online		
centralmarketing[.]store		
centralinvest[.]online		
centralmakermoney[.]online		
centralmakermoney[.]pro		
tiket-88[.]com		
tktiktok[.]shop		
tkokshop[.]com		
jar28[.]com		
je28[.]com		
universalmusicspace[.]com		
universal-onlinemusicservice[.]com		
universalproductiondosmusic[.]com		
universalpromohub[.]com		
universalwebplayer[.]com		
wikiwand-ppc[.]com		
wikiwand-works[.]com		
capitolmusicgroupboost[.]com		
capitolmusicpromohub[.]com		
capitolmusicpromotions[.]com		
capitolmusicwebplayer[.]com		
capitolrecords-music[.]com		
capitolrecords-works[.]com		
ppc-venture[.]com		
promohubventure[.]com		
venturemusic-data[.]com		
verse-one-ppc[.]com		
verse-one-data[.]com		
vertify-agency-dos[.]com		
verifyseoagency[.]com		
verifyppcagency[.]com		
winamppromohub[.]com		
warnermusicspace[.]com		
warnerwebplayer[.]com		
musicspace-rr-records[.]com		
webplayerrrrecords[.]com		

roadrunnerrecordsdata[.]com	
roadrunnerrecordsseo[.]com	
rr-musicalbumsdata[.]com	
rrrecords-ppc[.]com	
rrrecords-promo[.]com	
you42musicspace[.]com	
you42promohub[.]com	
dataintelligenceoptimal[.]com	
rcarecordsgroupboost[.]com	
rcarecordsgroupppromo[.]com	
rcarecordsmusicgroupboost[.]com	
rcarecordsmusicgroupppromo[.]com	
rcarecordsmusicpromohub[.]com	
rcarecordsmusicpromotions[.]com	
tiktok-advance[.]com	
madisontaylormarketingwork[.]com	
winampgrouphub[.]com	
temu-workbench[.]com	
mallsvip[.]vip	
tianmie[.]vip	
walmart-shopping[.]com	
musicplayerspoty[.]com	
attentivedata[.]com	
apm-player[.]com	
apm-space[.]com	
atom-tickets-data[.]com	
atom-tickets-ppc[.]com	
temu-get-work[.]com	
outlierventures-apps[.]com	
app-outlierventures[.]com	
apps-outlierventures[.]com	
outlierventures-app[.]com	

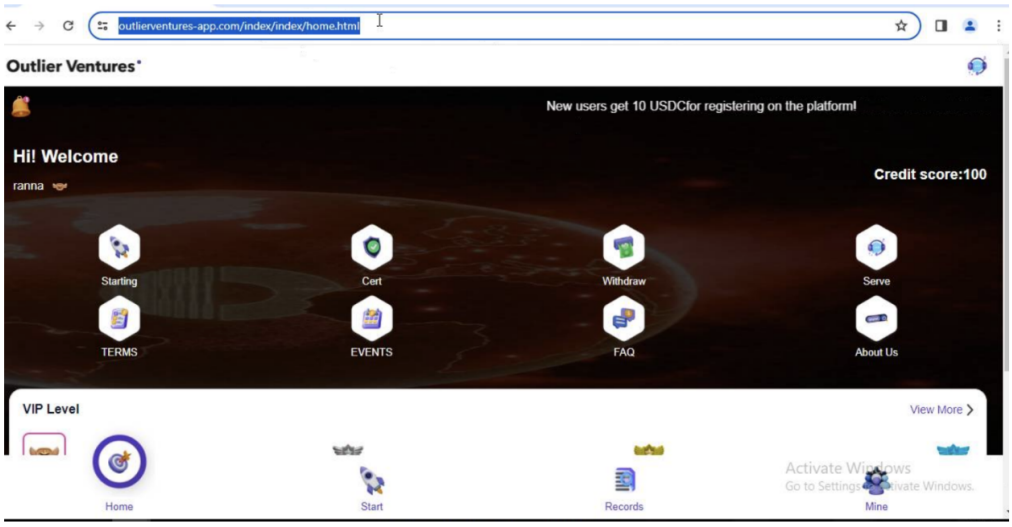
Appendix: Example screenshots of identified job fraud websites

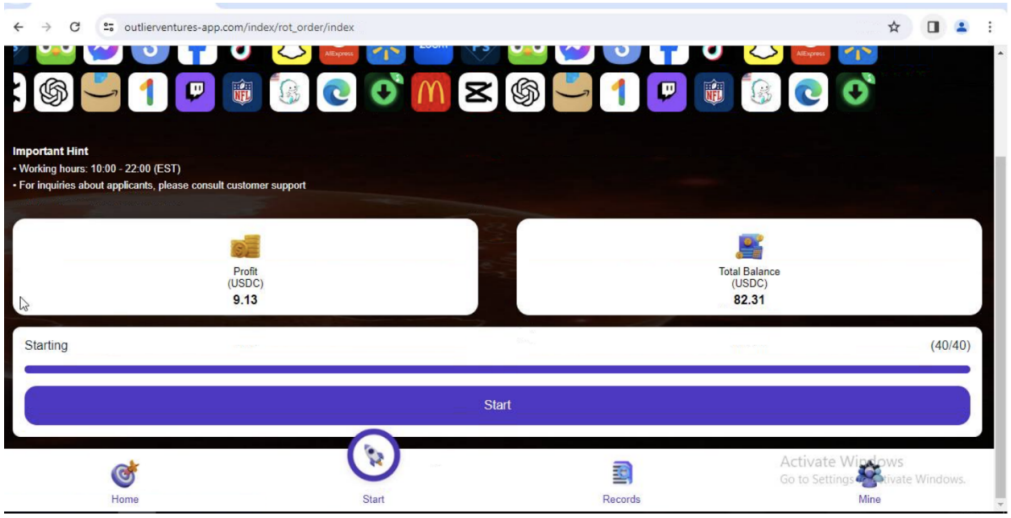
Here are some additional examples.

Fake hotel reviews on hotelassociationseogp[.]com

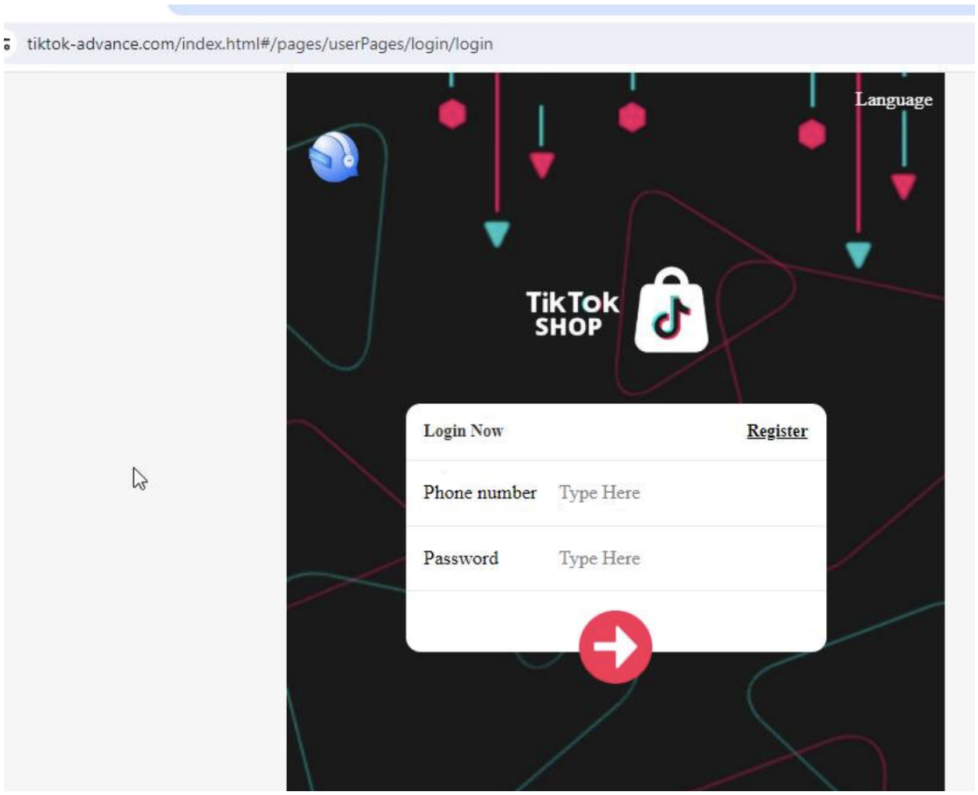


Fake app store reviews on outlierventures-app[.]com

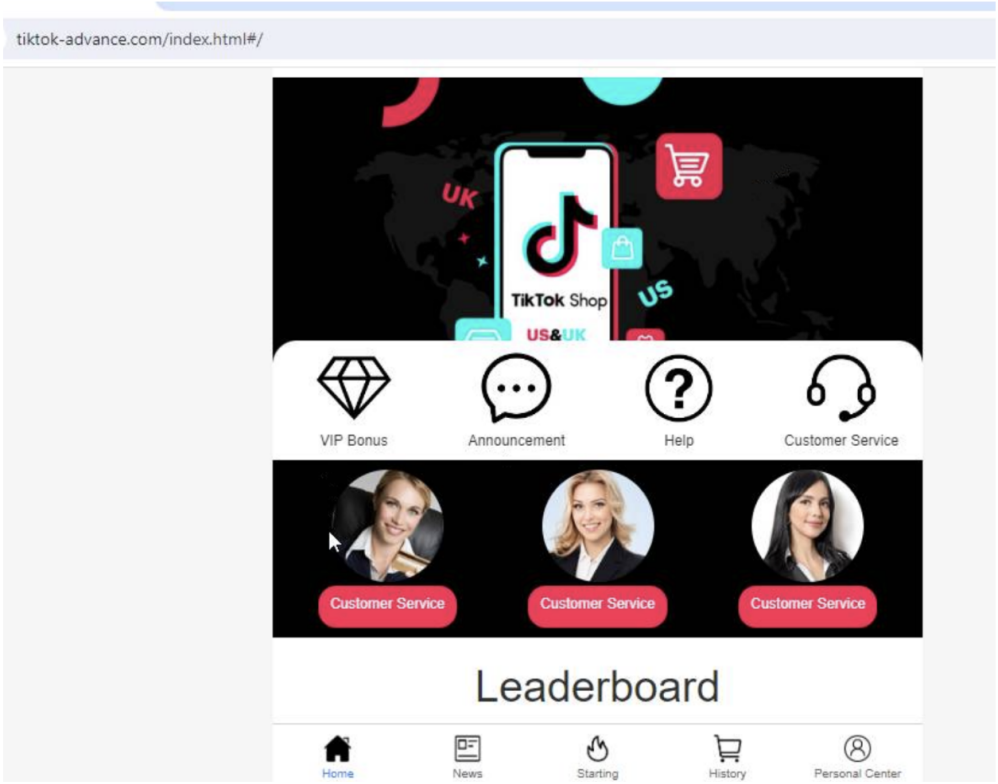


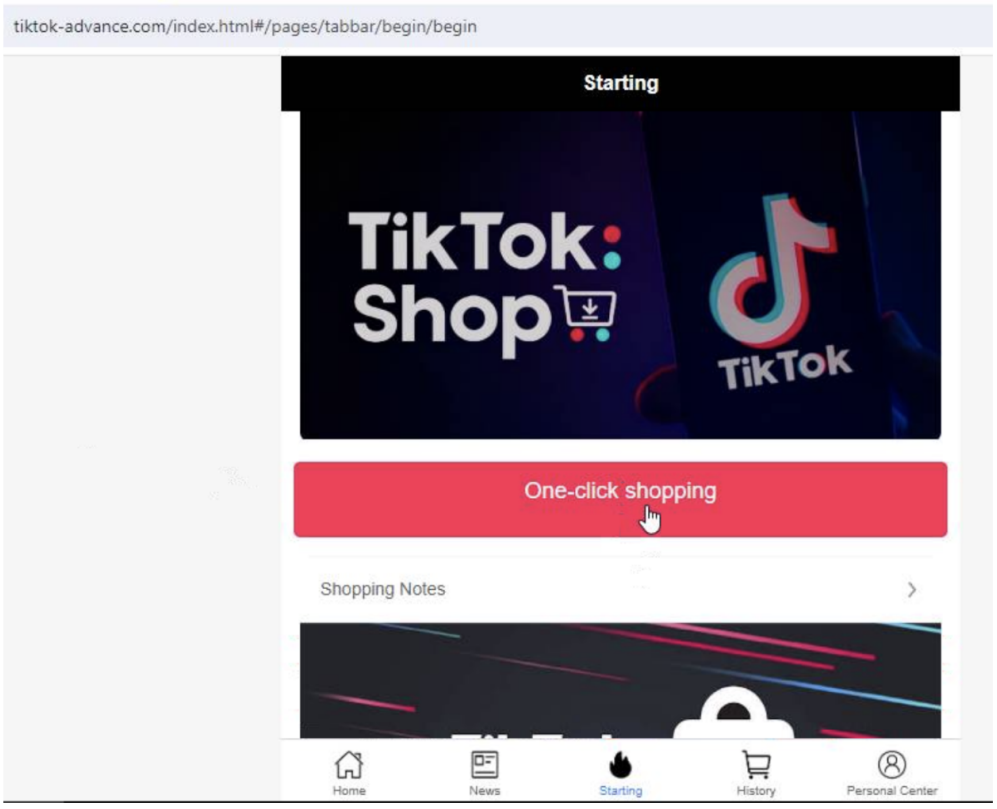


Fake TikTok shop reviews on tiktok-advance[.]com


tiktok-advance.com/index.html#/pages/userPages/login/login
Language
TikTok SHOP
Login Now
Register
Phone number
Type Here
Password
Type Here


TikTok Shop
Deposit Rewards Program
PLATFORM DEPOSIT REWARDS
DEPOSIT 500-1499
REWARD 5%
DEPOSIT 1500-4999
REWARD 7%
DEPOSIT 5000-9999
REWARD 10%
DEPOSIT >10000
REWARD 13%
PLATFORM SIGN IN BASIC SALARY
Get paid every 5 working days
1500USD





Subscribe to the Proofpoint Blog

Exhibit 1-B

Blockchain Tracing Report

Case Name:
Tracking Name:
Tracking ID:

Destination Address	Owner Name (Destination Address)	Stop Reason Additional information	Confirmed by all tracking methods	Blockchain	Asset Name	Assets Traced (average across all tracking methods; per Asset Type)	Assets Traced Inflow Start Time (across all tracking methods, UTC)	Assets Traced Inflow End Time (across all atracking methods, UTC)
22ce84a7f86662b78e49c6ec9e51d60fdde7b70a	Bitget	Exchange | Other Organization | Paym	Yes	ETH	USDCoin	100,800.01201200	2025-03-18 02:52:11	2025-03-18 02:57:11
c66aa76e224768e3f6beb6dcb31f9ad3abdf82a6	Coinbase	Exchange | Payment Service | Other C	Yes	ETH	USDCoin	20,000.00000000	2025-02-22 03:20:23	2025-02-22 03:20:23

Case Name: Steinhardt
Tracking Name: Steinhardt DOF ETH Tracking
Tracking ID: f74ce614-3571-4ccb-b1ca-9f680b9953d8

Transaction Hash	Owner Name (Destination Address)	Destination Address	Blockchain	Asset Name	Confirmed by all tracking methods	Transaction Date (UTC)	Assets Traced (average across all tracking methods; per Asset Type)
b4f1c7058ea35690087114f5058ab5b381ce190f8dc072ff6504e722beceec7e	Bitget	22ce84a7f86662b78e49c6ec9e51d60fdde7b70a	ETH	USDCoin	Yes	2025-03-18 02:52:11	50,000.00000000
6d1305207103561117cb450ef12362e104722ba8186bfd8f4382277713705c0a	Bitget	22ce84a7f86662b78e49c6ec9e51d60fdde7b70a	ETH	USDCoin	Yes	2025-03-18 02:57:11	50,800.01201200
4cfa7699ade24901b9ae36b6c40fe93b0fb1e8936ac9b676e67ad54df050b92d	Coinbase	c66aa76e224768e3f6beb6dcb31f9ad3abdf82a6	ETH	USDCoin	Yes	2025-02-22 03:20:23	20,000.00000000

Exhibit 1-C

Blockchain Tracing Graph